ماژول امنیت سخت‌افزاری (HSM) صدف

مشخصات فنی صدف

مشخصات فنی ماژول امنیت سخت‌افزاری صدف	
مرز حفاظت سخت‌افزاری	پیاده‌سازی و اجرای کلیه عملیات حساس امنیتی در داخل سخت‌افزار: • مدیریت کلید (تولید، حفاظت، پشتیبان‌گیری و بازیابی) • عملیات رمزنگاری/تولید امضا/تصدیق اصالت
سطح امنیتی	قابل پیکربندی در دو سطح: • FIPS 140-2 Level 2 • FIPS 140-2 Level 3 دارای «گواهی‌نامه امنیتی FIPS 140-2 Level 3» از «مرکز دولتی صدور گواهی الکترونیکی ریشه»
حفاظت فیزیکی	• تشخیص دستکاری فیزیکی (Tamper Evidence) و پاسخ به آن (Tamper Response) با استفاده از سنسورهای حفاظت فیزیکی • اعمال حفاظت فیزیکی بر اساس استاندارد FIPS 140-2 Level 3/4 • مجهز به باتری قابل تعویض از بیرون (توسط مشتری)
رمزنگاری نامتقارن	RSA (1024, 2048, 4096) • Padding: PKCS#1v1.5, PKCS#1v2.2 (OAEP, PSS) ECDSA • SECP256R1, SEC256K1, SECP384R1 • BrainpoolP256R1,BrainpoolP384R1,BrainpoolP512R1, BrainpoolP512T1
رمزنگاری متقارن	AES (128, 192, 256) • Modes: ECB, CBC, OFB, CFB, CTR, GCM DES (56), TDES (112, 168) • Modes: ECB, CBC, OFB, CFB
Hash Functions	MD5 SHA-1 SHA-2 (224, 256, 384, 512)
MAC Algorithms	HMAC (MD5, SHA-1, SHA-2) CMAC (AES, TDES) MAC [ANSI X9.9] (AES, DES, TDES) MAC [ANSI X9.19] (AES, TDES)
Wrap/Unwrap Algorithms	Symmetric Wrap/Unwrap (NIST SP 800-38F) Symmetric Wrap/Unwrap (AES/DES/TDES) Asymmetric Wrap/Unwrap (RSA, PKCS#8)
پشتیبان‌گیری/بازیابی امن	Cloning (HSM to HSM) Manual Synchronizatoin (among multiple HSMs) Partition Backup (HSM to USB Token) M_of_N Secret Sharing (HSM to Multiple USB Tokens)
تولید عدد تصادفی	Hardware-based True Noise Source NIST SP 800-90A compliant CTR-DRBG
پشتیبانی از پیاده‌سازی الگوریتم‌های رمزنگاری یا پروتکل‌های امنیتی بومی/اختصاصی روی سخت‌افزار	

مشخصات فنی ماژول امنیت سخت‌افزاری صدف	
مشخصات فنی متناظر با حوزه پرداخت (Payment)	
کلیدها و الگوریتم‌های رمزنگاری مورد نیاز در تضمین امنیت پیام‌های شبکه شتاب	بر اساس «مستندات فنی شتاب» و «استاندارد ISO8583» PIN Protection/Translation ANSI X9.19 MAC Generation/Verification CSD Protection
انواع PIN Block (شامل ISO Format 4 و ISO Format 0/ANSI X9.8)	• پشتیبانی از الگوریتم‌های پایه مورد نیاز • سفارشی‌سازی بر اساس نیازمندی‌های عملکردی مشتری
تولید و وارسی PIN Verification Value (PVV) و Card Verification (CVV2) Value	• پشتیبانی از الگوریتم‌های پایه مورد نیاز • سفارشی‌سازی بر اساس نیازمندی‌های عملکردی مشتری
EMV Transaction Processing	• پشتیبانی از الگوریتم‌های پایه مورد نیاز • سفارشی‌سازی بر اساس نیازمندی‌های عملکردی مشتری
صدور کارت / کارت هوشمند	• صدور SIM Card (همراه اول و تالیا) • سفارشی‌سازی بر اساس نیازمندی‌های مشتری برای صدور کارت با سایر کاربردها (شامل کارت هوشمند ملی، بانکی و سوخت)
کاربران/نقش‌ها	+ Multiple Administrators per HSM Device + Separate Administrator account for Audit operations + Two distinct Users per HSM Partition: • Security Officer • Normal User
تصدیق اصالت	FIPS Level 2 • Secure Password-based Authentication FIPS Level 3: • Secure USB Token-based Authentication (PED-based Trusted Path, Two-Factor Authentication, M-of-N Login)
Logging / Audit	Syslog, SIEM
پروتکل ارتباطی	• مدیریت HSM مبتنی بر SSH • کاربری HSM مبتنی بر TLS • ارتباط با PIN Entry Device (PED) مبتنی بر TLS
API	• PKCS#11 • Java JCA/JCE • .NET Wrapper • OpenSSL Engine • Microsoft CNG (KSP)
سیستم عامل	Linux / Unix,Windows

مشخصات فنی ماژول امنیت سخت‌افزاری صدف			
Algorithm	**LAVAN**	**KISH**	**کارایی (TPS)**
RSA 1024	4500	4500	**RSA Sign/Sec**
RSA 2048	900	2200	
RSA 4096	170	350	
AES 256	8000	12000	**Symmetric Enc/Sec**
DES/TDES	8000	12000	
RSA 1024	1 sec	1 sec	**RSA KeyPair Generation Time**
RSA 2048	3 sec	3 sec	
RSA 4096	20 sec	20 sec	
پشتیبانی از High Availability (HA) **Active-Active Failover** **Loadbalancing**			
پشتیبانی از Network Time Protocol (NTP)			
• Network Access Control Rules • SNMP			**Network Management**
+ 1U Rack Mount + Dual Hot-Swap Power Supply + Ethernet port (1 Gbps) + USB and Serial ports (for HSM Management) + LED (Power, Tamper) + LCD + PED (PIN Entry Device)			**مشخصات فیزیکی، واسطها و پورت‌های ارتباطی**
+ Web/Application Server (HTTPS/SSL/TLS) • Weblogic • Tomcat • NGINX • Apache • IIS + Database Security, Transparent Data Encryption • Oracle • PostgreSQL + Network Security • OpenVPN • Bind DNS Server (DNSSec) + Application Security • HashiCorp-Vault • PKI: Windows Certificate Server/Authority • OTA (Over-The-Air), Advanced OTA • Secure Email: Mozilla Thunderbird			**پشتیبانی از برنامه‌های کاربردی**